Appendix 7

Restoration Strategy for Centrally Administered Information Resources

Background

The Information Technology Division has developed and maintains an Information Resources Disaster Recovery Plan (DRP) to facilitate immediate response to unplanned disruptions in information technology services, such as those resulting from utility outages, damage to data center facilities, and even campus-wide disasters. The DRP is designed to operate in standalone recovery situations or in concert with the university's Disaster/Emergency Operations policies and procedures (UPPS 05.04.03) and Business Continuity Plans (BCPs). Departments may wish to use this strategy statement as a reference when developing their departmental BCPs.

The university presently maintains two data centers on the San Marcos campus that provide near hot-site redundancy for each other with respect to mission critical applications and services. The data centers are connected to each other and to the Internet via two separate fiber network circuits over separate pathways in a fiber ring. The data centers are not complete "hot sites" for each other, but provide a high level of redundancy in processing capacity, disk storage, and backup resources for mission critical services. Given this network architecture, the DRP was developed under four basic planning assumptions. The plan assumes that:

1. human health and safety priorities have been addressed and that IT recovery teams can complete their tasks in a relatively safe environment;
2. the highest IT priority is restoration of the mission critical, technology infrastructure required to support centrally administered voice/data communications and one or both centrally administered data centers;
3. outages in even the most critical systems (e.g., payroll, procurement, registration) do not become critical until they (are expected to) last longer than 48 hours; and
4. the concurrent loss of both university data centers in a single disaster event is much less likely than the loss of a single data center and that either data center is capable of supporting mission critical IT services, with limited service degradation, until the damaged data center is fully recovered.

IT Service Restoration Priorities

Consistent with the university plans and planning assumptions referenced above, the Information Technology Division's service restoration priorities are as follows.

Priority 1: Assess damage and restore core infrastructure in the university data centers and other critical network locations. Examples of core infrastructure include physical voice/data network connectivity to the Internet and between the data centers, as well as reliable electrical power, environmental (HVAC) controls, and physical security in the data centers and other critical equipment locations, etc.

Priority 2: Restore critical communication systems, including land-line and wireless telephone services to key locations, electronic mail and related services, GATO Web services, and key components of campus emergency notification systems, etc.

Priority 3: Restore centrally administered applications and services, and user access to those applications and services, according to the priority groups shown in Table 1 below. Restoration will proceed in priority group order, starting with priority group 1 and continuing through priority group 4. Table 2 reflects these same applications as they are presented in Step III. Information Technology within the Texas State Ready BCP tool.

Priority 4: Restore any remaining applications and assist departments with unresolved information technology issues.

Departmental Restoration Priorities

In Step III. Information Technology of the Texas State Ready BCP tool, each department will identify centrally administered systems that it deems critical to departmental functions. The department will assign a Level of Criticality for each identified system based upon the department's maximum tolerable outage period and the following scale:

Critical 1: Department can function without application for up to 48 hours.
Critical 2: Department can function without application for up to 10 calendar days.
Critical 3: Department can function without application for up to 30 calendar days.
Critical 4: Department can function without application for more than 30 calendar days.

Table 1 on the following pages represents an initial grouping of the applications based upon IT's current perception of the mission criticality of each application to the university as a whole. An application may be moved to a different priority group if subsequent analysis of completed departmental BCPs suggests a different criticality level for the application.